Chapter 6: Logging In from Off-Site

In this chapter, we discuss what off-site users are required to do in order to access Fermilab's strengthened realm, and some of the issues they may encounter.

Due to practical considerations, namely the fact that off-site machines at universities may be shared by many people, some of whom do not access Fermilab at all, off-site users are not required to install a Kerberos 5 server. Off-site machines participating in Fermilab's strengthened realm have a choice of authentication methods, including ssh with passwords, public/private keys, host-based keys or Kerberos. Access to a system on-site at Fermilab requires Kerberos credentials or a CRYPTOCard.

6.1 Description of Choices for Off-Site Machines

The choices for off-site machines include:

1) Install the Kerberos client (and optionally the Kerberized ssh client) software on your machines and sign up to be part of the FNAL.GOV strengthened realm. This means you can authenticate to Kerberos locally and connect to Fermilab computers using the Kerberized version of a network connection program. This is the preferred method.

2) Leave your machines unstrengthened and always log in to Fermilab using your CRYPTOCard (see Chapter 5: *Using your CRYPTOCard*). Note that if you choose to do this, we recommend that you use ssh as the transport program in order to ensure encryption. You must NEVER type in your password if you are on an unencrypted channel! There is no way to perform any Kerberos command that requires a password while logged in using an X-terminal. And please, as much as possible, refrain from performing operations that involve typing your Kerberos password over the network.

3) Your site may have its own version of strong authentication which may be acceptable to Fermilab and then you could become a trusted realm.

4) In addition, a stripped-down kerberos product exists for emergency off-site use, e.g., for people who've misplaced their CRYPTOCard. It is called **FNAL-kerberos-clientonly** and is described in section 6.2 *In a Pinch: Download Client-Only Version of Kerberos*. This product is intended for temporary use. People using the same machine repeatedly will likely find a full Kerberos installation more useful and convenient.

The Cryptography Publishing Project is making MIT Kerberos V5 release 1.2.1 available for export without restriction (software for Macintosh excepted); see `http://www.crypto-publish.org/`.

If people need to log in from your site to change their passwords, there must be at least one local machine on which there is software which will allow it to be done locally (best) or over an encrypted connection (second best).

6.2 In a Pinch: Download Client-Only Version of Kerberos

New as of June 2002:

FNAL-Kerberos-clientonly is a stripped-down version of Fermi Kerberos containing only the client applications and supporting files needed to connect to an FNAL Kerberized machine from a remote location. It is intended for temporary use by off-site users who have neither a CRYPTOCard nor a machine with a Kerberos installation available. **FNAL-Kerberos-clientonly** is publicly-available, it is provided in tar format, it can be downloaded via a web browser and installed in any user directory, and it does not require root/administrator privileges to operate.

FNAL-Kerberos-clientonly versions have been created for RedHat Linux 7.1 and compatible systems, and for Windows 2000 (other Windows systems have not been tested but may work). Look for the software in the FermiTools area of Fermilab's FTP server: `ftp://ftp.fnal.gov/pub/fnal-kerberos-clientonly/current/`. Instructions on how to setup and uninstall the software are included in the product.

6.3 Obtaining CRYPTOCards

All users, on-site and off-site, can request a CRYPTOCard using the *Request Form for Computing Username and Primary Accounts* at `http://www.fnal.gov/cd/forms/acctreq_form.html`. If you

visit Fermilab occasionally, come by WH8NE to pick it up when it's ready. For those experimenters or other users who will not be visiting Fermilab, CRYPTOCards can be mailed. Each group or experiment should have a person designated to mail CRYPTOCards; contact the appropriate person to request mailing.

If you lose your CRYPTOCard or it becomes unusable for any reason, please email *compdiv@fnal.gov* or call Yolanda Valadez at 630-840-8118 to request a new one. Then ask the person designated for your group or experiment to pick it up from her and mail it to you. Currently we do not have a way of restoring your access more quickly. By the end of 2001, we expect to have a mechanism in place whereby we can fax you a one-time password.

6.4 Exporting CRYPTOCards

For users outside the U.S., you can carry a CRYPTOCard back to your home or institution with no customs problems since the cards are for authentication, not encryption. They can be mailed outside the U.S., too.

6.5 Network Address Translation

There is an issue concerning users who maintain a small network of computers at home and whose ISP subjects them to NAT (Network Address Translation). Typically, the user dials up with a NAT box or a Linux host configured to do NAT for the house network, and receives one address from his or her ISP. This address may be static or dynamic. In either case, NAT can make it difficult or impossible to authenticate over the network to the FNAL.GOV realm.

There are a couple of solutions, one of which is to keep your home machines unKerberized, and use a CRYPTOCard. If you want to Kerberize your home machines, we would first recommend that you change ISPs to one that eschews NAT. Barring that, you may be able to work around NAT:

- *if* your home machines (Linux or Macintosh) have **kerberos** installed,
- *if* there is a single fixed "public" IP address associated with your machines' real IP addresses, and the outside world sees this public IP address as the source of packets that come from your machines,
- and *if* you can determine this fixed IP address.

To be able to authenticate, you'd need to include this public IP address in your local `/etc/krb5.conf` file under the `[libdefaults]` section as: `proxy_gateway = <fixed.IP.address>`. If the address is dynamic, this solution will rapidly become annoying, no doubt.

We recommend that you use ssh to connect to the lab. Kerberized ssh is of course best, but any ssh with CRYPTOCard works too (only one CRYPTOCard use per remote host, not per window). Because ssh includes an automatic tunnel for X sessions, most users will find this more convenient than telnet/rlogin connection methods.

6.5.1 Windows

If you've installed **WRQ®** on your Windows system(s), you will not be able to authenticate if your ISP uses NAT. Remove this software from your system(s) and use a CRYPTOCard. The vendor is aware of this problem, and may address it in future releases of the software.

In the meantime, you can use a combination of an ssh client (e.g., F-secure) with Exceed or the Reflection X Manager (but make sure your site is not behind a firewall in addition to NAT).

6.5.2 Linux

If you install Linux, configure your machine such that its hostname is equivalent to the external hostname your ISP uses, then install a Kerberos client. (If you're not sure how to configure, send an email to *kerberos-users@fnal.gov*, or check the archives.)

6.5.3 Macintosh

To enable **BetterTelnet** to work for a Kerberized Macintosh in a NAT environment, you must add the following line to the `libdefaults` section of the `Kerberos Preferences` file (Note that this reduces the security of your Kerberos credentials.):

```
noaddresses = true
```

Forwardable tickets to do not work. Opening a connection with **BetterTelnet** results in a dialog box from the Kerberos5 Telnet Plugin about the forwarded credentials being refused due to bad address. Clicking **OK** will result in the telnet connection opening as expected, otherwise.